Politica di divulgazione coordinata delle vulnerabilità

Coordinated Vulnerability Disclosure (CVD) dei prodotti Connee

Codice	CRA-D3
Versione	1.0 del 25/11/2026
Titolare	Nicola Preo, CTO (sostituto: Marco Migozzi, Tech Lead)
Classificazione	Pubblico
Riferimenti	Reg. (UE) 2024/2847 All. I parte II p. 5-6; ENISA Technical Advisory ott. 2026; RFC 9116

1. Impegno

Connee S.R.L. accoglie le segnalazioni di vulnerabilità nei propri prodotti, le gestisce in modo riservato e pubblica le correzioni in modo coordinato con chi segnala.

2. Ambito

Incluso	Note
App Connee (iOS, Android)	Tutte le versioni nel periodo di assistenza
Connee Component per Home Assistant	Integrazione installata sull'HUB del cliente
Connee Control Room	Servizio cloud collegato al Connee Component (assistenza, OTP)
Ajax Systems by Connee	Integrazione HA + gateway cloud Connee
Connee Monitor / Solar Guardian	Integrazione HA + servizio cloud Solar Guardian

Escluso: prodotti di terzi (Home Assistant, HUB, Ajax, LuxPower), da segnalare al rispettivo produttore. Se la vulnerabilità di terzi impatta un prodotto Connee, Connee coordina con il produttore (art. 13(6) CRA). Esclusi anche: DoS, spam, ingegneria sociale, accesso fisico, report automatici senza impatto dimostrato, sito web istituzionale.

3. Come segnalare

- Canale unico: modulo su **https://conneehome.com/it/security**.
- Ogni segnalazione riceve un numero di pratica (SEC-AAAA-NNNN) e una ricevuta via e-mail.
- Lingue: italiano, inglese.
- Contatto e politica sono pubblicati anche in /.well-known/security.txt.

4. Regole di test

- Solo su account e dispositivi propri.
- Nessun accesso, modifica o cancellazione di dati altrui; se si accede per errore a dati di terzi: interrompere e segnalarlo.
- Nessuna interruzione o degrado del servizio.
- Nessuna divulgazione prima della correzione concordata.

5. Informazioni richieste

Campo	Obbligatorio
E-mail di contatto	Sì
Prodotto e versione	Prodotto sì, versione se nota
Descrizione e passi per riprodurre	Sì
Sfruttata attivamente (sì/no/non so)	Sì
Tipo, impatto stimato, link a proof of concept	No

6. Cosa aspettarsi

Fase	Tempo obiettivo
Conferma di ricezione	Entro 2 giorni lavorativi
Valutazione e gravità (CVSS 3.1)	Entro 7 giorni
Aggiornamenti al segnalante	Almeno ogni 14 giorni
Correzione e divulgazione	Entro 90 giorni; prima se sfruttata attivamente

Se la vulnerabilità risulta sfruttata attivamente, Connee la notifica a CSIRT Italia ed ENISA tramite la piattaforma unica di segnalazione nei termini dell'art. 14 CRA (24 h / 72 h / 14 giorni).

7. Tutela legale

Connee non intraprende azioni legali contro chi segnala in buona fede rispettando questa politica. La tutela vale solo per i sistemi Connee e non autorizza test su sistemi di terzi.

8. Divulgazione coordinata

- Embargo fino alla correzione disponibile o fino a 90 giorni, salvo accordo diverso.
- Condivisione solo con chi deve correggere (es. produttore del componente di terzi).
- Pubblicazione: avviso CSA-AAAA-NNN su https://conneehome.com/it/security con CVE, gravità, versioni colpite e corrette, rimedio.
- Gli aggiornamenti di sicurezza sono gratuiti per tutto il periodo di assistenza.

9. Riconoscimenti

Nessun programma a premi. Eventuali citazioni solo con consenso esplicito del segnalante.

10. Dati personali e riservatezza

I dati del segnalante sono trattati solo per gestire la segnalazione, secondo l'informativa privacy di Connee, e non sono condivisi senza consenso salvo obblighi di legge (es. notifiche CSIRT/ENISA).

11. Gestione della politica

- Titolare: Nicola Preo (CTO). Sostituto: Marco Migozzi (Tech Lead).
- Revisione: annuale o a ogni modifica di prodotti, processi o norma.
- Titolare/contatto Connee S.R.L., Viale Cristoforo Colombo 23, 70017 Putignano (BA), CF e P.IVA 08954930726.

Storico revisioni

Versione	Data	Autore	Modifica
1.0	25/11/2026	Nicola Preo, CTO (sostituto: Marco Migozzi, Tech Lead)	Prima emissione